PCT/IB 03/04190
19.09.03

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

#2

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

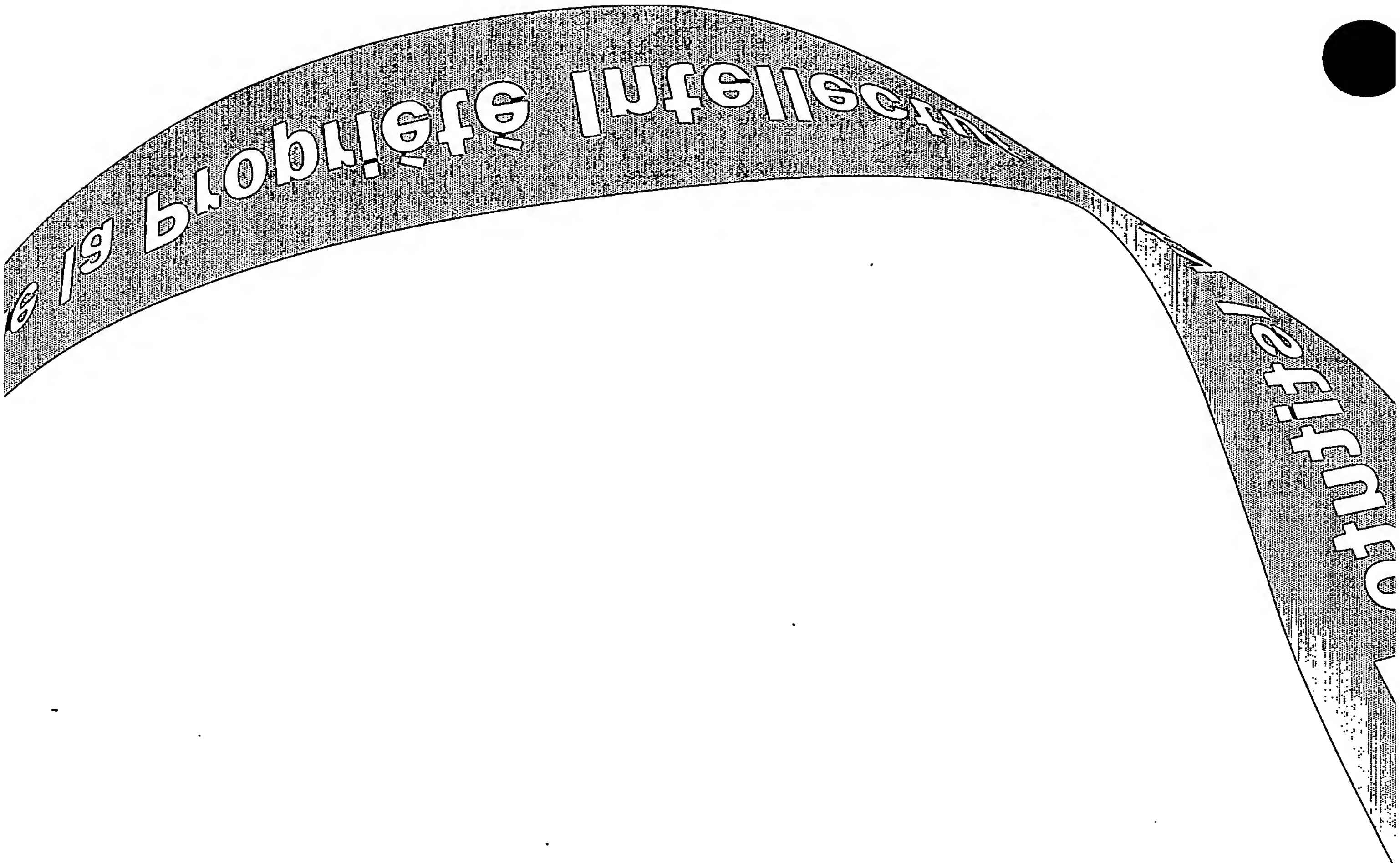
I documenti allegati sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 27. AUG. 2003

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione dei brevetti

H. Jenni
Heinz Jenni



Demande de brevet no 2002 1605/02

CERTIFICAT DE DEPOT (art. 46 al. 5 OBI)

L'Institut Fédéral de la Propriété Intellectuelle accuse réception de la demande de brevet Suisse dont le détail figure ci-dessous.

Titre:
Méthode de contrôle d'appariement multiple.

Requérant:
Nagracard S.A.
22, route de Genève
1033 Cheseaux-sur-Lausanne

Mandataire:
Leman Consulting S.A.
Rte de Clementy 62
1260 Nyon

Date du dépôt: 24.09.2002

Classement provisoire: H04N

METHODE POUR LE CONTROLE D'APPARIEMENT MULTIPLE

La présente demande concerne le domaine de l'appariement entre un module de sécurité et un module hôte, notamment afin de sécuriser les communications entre ces deux modules.

L'appariement est un mécanisme connu qui consiste à partager un secret unique à deux dispositifs rendant la communication ente ces deux dispositifs inaccessible pour tout autre dispositif.

Cet appariement est décrit dans la demande EP1078524 et permet de lier un module de sécurité à un récepteur grâce à la présence d'une clé de chiffrement unique connue de ces deux seuls éléments.

Dans un environnement autorisant la connexion d'un module de sécurité sur plusieurs appareils hôtes, un tel appariement n'est pas possible car trop limitatif.

Le document WO02/052515 décrit une solution mettant en œuvre le contrôle de l'appariement par un centre de gestion. Le module de sécurité peut être apparié à n'importe quel appareil pour autant que le centre de gestion l'y autorise. Une telle solution suppose l'existence d'un canal permettant au centre de gestion d'adresser un ou plusieurs messages au module de sécurité.

Le but de la présente invention est donc d'apparier un module de sécurité avec un ou plusieurs appareils hôtes dans un environnement dans lequel soit l'appel à un centre de gestion n'est pas possible lors de l'appariement, soit aucun canal n'existe entre le centre de gestion et le module de sécurité.

Ce but est atteint par une méthode de contrôle d'appariement entre un premier dispositif tel qu'un module de sécurité amovible et un second dispositif tel qu'un appareil hôte, cet appariement consistant à sécuriser

l'échange des données à l'aide d'une clé d'appariement unique, cette méthode consistant à :

- vérifier l'appariement entre les deux dispositifs et utiliser la clé d'appariement unique si l'appariement est déjà effectué, dans la négative,

- rechercher un emplacement vide parmi les emplacements réservés aux données d'appariement dans le premier dispositif et dans l'affirmative,

- initier une procédure d'appariement en transmettant un cryptogramme contenu dans le second dispositif, et contenant un identifiant propre à ce dispositif, ce cryptogramme étant encrypté par une clé secrète commune à tous les premiers dispositifs,

- décrypter par le premier dispositif ce cryptogramme et en extraire l'identifiant du second dispositif,

- générer une clé d'appariement basée sur cet identifiant,

- mémoriser dans le premier dispositif les données de l'appariement avec le second dispositif.

Deux caractéristiques importantes sont contenues dans cette méthode. La première est la possibilité de mémoriser dans le module de sécurité (premier dispositif) plusieurs données d'appariement. Le nombre maximum sera volontairement limité pour empêcher qu'un même module puisse s'apparier avec un nombre illimité d'appareils hôtes.

La deuxième caractéristique est la manière de créer la clé d'appariement. A l'origine, rien ne destine un module de sécurité particulier à s'apparier avec un appareil hôte particulier. C'est pourquoi, selon une première variante, un identifiant unique de l'appareil hôte (second dispositif) est encrypté par une clé qui est contenue dans

chaque module de sécurité. Cet identifiant peut être le numéro de série de l'appareil hôte ou une clé de chiffrement ou un numéro généré aléatoirement lors de la personnalisation de chaque appareil hôte ou encore un mélange de ces éléments.

Selon un mode de réalisation, le cryptogramme contient une clé secrète qui peut être de type symétrique ou asymétrique. Une fois déchiffré par le module de sécurité, ce dernier génère une clé aléatoire qui sera la clé d'appariement et l'encrypte avec la clé secrète puis l'envoie à l'appareil hôte. Le numéro de série unique de l'appareil hôte sera de préférence contenu dans les premiers messages échangés entre les deux éléments pour effectuer la vérification de l'appariement.

Selon une deuxième variante, la clé d'appariement est déjà contenue dans le cryptogramme transmis par le deuxième dispositif. Dans un tel cas, la clé d'appariement est une clé unique, propre à l'appareil hôte et ne dépend en rien du module de sécurité

L'invention recouvre également un mode dans lequel le cryptogramme est contenu dans le module de sécurité. C'est ce dernier qui va transmettre le cryptogramme à l'appareil hôte pour la génération de la clé d'appariement. On considère que la clé de déchiffrement commune stockée dans ce cas dans l'appareil hôte est stockée dans un élément de sécurité, tel qu'une mémoire sécurisée.

Si un nouvel appariement est effectué, les données d'appariement seront enregistrées et occuperont un des emplacements prévus pour les différents appariements que peut accepter un module de sécurité. Les données d'appariement sont par exemple le numéro de série de l'appareil hôte accompagné de la clé d'appariement.

Du fait que le nombre d'emplacements est limité, il est probable que le module de sécurité soit connecté avec un nouvel appareil hôte alors

que tous les emplacements sont utilisés. Pour déterminer l'emplacement à remplacer, il existe plusieurs mécanismes à savoir:

- un compteur d'activité associé à chaque emplacement. A chaque négociation d'appariement entre le module de sécurité et l'appareil hôte, ce compteur est incrémenté. Ainsi, le plus petit compteur détermine l'emplacement le moins utilisé. C'est cet emplacement qui sera remplacé par le nouvel appariement. Par négociation d'appariement, on entend en général la mise sous tension du module hôte et la requête d'information de la part du module de sécurité.

- un compteur de chronologie d'appariement associé à chaque emplacement. A chaque négociation d'appariement, le compteur correspondant prend la valeur du plus haut de tous les compteurs plus un, sauf si ce compteur est déjà le plus haut, auquel cas il n'est pas modifié. Ainsi, le compteur ayant la plus petite valeur indique l'emplacement de l'appariement le plus ancien. C'est cet emplacement qui sera remplacé par le nouvel appariement.

Dans une forme de réalisation, tout nouvel appariement ou tout changement d'appariement (ceci survenant lorsqu'il n'y a plus d'emplacement libre) est sujet à l'introduction d'un code secret (PIN code). A la première insertion du module de sécurité dans l'appareil hôte, le module de sécurité initie une séquence auprès de l'appareil hôte qui selon ses moyens d'affichage, demande à l'utilisateur l'introduction de ce code secret. Ce n'est que si ce code est correctement fourni par l'utilisateur, puis transféré vers le module de sécurité, que ce dernier acceptera ce nouvel appariement.

Selon les variantes choisies, il est possible d'exiger ce code secret pour chaque nouvel appariement sans relation avec l'occupation des emplacements de la mémoire. Dans une autre variante, il est possible

de faire intervenir le code secret lorsqu'il est question de remplacer un emplacement déjà occupé.

Plusieurs variantes sont prévues pour déterminer la validité de ce code secret. Dans une première variante simplifiée, le code secret est constant pour un module de sécurité et est distribué avec ledit module.

Dans une deuxième variante, l'utilisateur appelle ou se connecte à un centre de gestion et lui transmet le numéro unique du module de sécurité et de l'appareil hôte. Ce centre calcule un code secret selon un algorithme prenant en compte les deux variables que sont les deux numéros uniques. Cet algorithme est également contenu dans le module de sécurité pour vérifier la conformité du code secret. L'appel au centre de gestion peut s'effectuer préalablement à l'appariement afin de disposer du code nécessaire lorsqu'il sera requis au moment de la connexion du module avec l'appareil hôte.

Selon une troisième variante, l'algorithme utilisé pour le calcul du code est basé sur le numéro unique du module de sécurité et d'un indice incrémental. Ce code est ensuite combiné avec le numéro unique de l'appareil hôte afin d'obtenir le code secret qui est ensuite transmis à l'utilisateur pour autoriser son nouvel appariement.

Le code peut être déterminé selon la formule : $CS = G(K , (F^N(UA))) = G(K , F((F^{N-1}(UA))))$, ou CS est le code secret, UA le numéro unique du module de sécurité, N l'indice incrémental, K le numéro unique de l'appareil hôte, F une fonction de chiffrement et G une fonction qui fait intervenir K dans le calcul du CS.

De cette manière, le code secret change inévitablement à chaque appariement. Soit le résultat de la fonction $F^{N-1}(UA)$, soit la valeur de l'indice N est stocké en mémoire du module pour être utilisée comme départ lors du prochain appariement. Pour que le centre puisse calculer

le bon code secret, il est nécessaire que le centre soit synchronisé avec le module de sécurité. Pour ce faire, l'utilisateur, lors de la requête, peut, par exemple, communiquer au centre la valeur de l'indice N ou le résultat de la fonction $F^{N-1}(UA)$, préalablement transmis par le module de sécurité. Bien entendu, l'utilisateur doit aussi transmettre le numéro unique du module de sécurité et de l'appareil hôte au centre de gestion.

Néanmoins, si la valeur de l'indice N dans le module de sécurité n'est pas accessible au centre de gestion, ce dernier peut transmettre un code secret qui ne corresponde pas nécessairement au dernier indice du module de sécurité. Suite à cet éventuel décalage entre l'indice stocké dans le module de sécurité et l'indice stocké au centre de gestion, un code secret correctement calculé au centre de gestion peut être rejeté par le module de sécurité.

Dans ce cas, il est possible de resynchroniser le module de sécurité. Si par exemple, le centre de gestion a fourni un code secret à partir du numéro de l'appareil hôte de l'utilisateur et du cryptogramme d'indice incrémental 12, soit celui qui est dans le centre de gestion, et si le cryptogramme mémorisé dans le module de sécurité est d'indice 8, alors le module va calculer les codes secrets correspondants aux indices 8, 9, 10, 11, 12 pour constater que le cryptogramme provenant du code introduit manuellement correspond à un cryptogramme valide d'indice plus élevé. Cette constatation signifie que le centre de gestion a auparavant délivré quatre codes secrets que l'utilisateur du module de sécurité n'a finalement pas utilisé.

Il est certain que la différence d'indice entre l'indice courant (8 dans notre exemple) et l'indice du centre de gestion (12 dans notre exemple) sera limitée à un nombre acceptable. Il n'est pas question de balayer les milliers de possibilités dans l'espoir de trouver le bon code secret.

A noter que cette troisième variante inclut la possibilité de ne pas faire intervenir le numéro unique de l'appareil hôte dans le calcul du code secret, en définissant CS = (F^N(UA)) qui correspond au cas où la fonction G précédemment citée est définie par G(x,y) = y. Cette variante est intéressante si l'on souhaite séparer le code secret du numéro de l'appareil hôte. En effet, s'il est aisé de connaître le numéro du module de sécurité, par définition, un module aisément transportable, il est plus difficile de connaître le numéro unique de l'appareil hôte, en particulier si l'on doit obtenir le code secret avant de connecter les deux éléments.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère à la figure unique qui est donnée à titre d'exemple nullement limitatif, et qui illustre les deux éléments principaux et les données qu'ils contiennent.

Le module de sécurité MS comprend une base de données DB sécurisée dans laquelle se trouve entre autre les données d'appariement. Ces données référencées PDT1 à PDTn occupent les places mémoires 1 à n. Noter que le nombre n d'emplacements prévus dans le module MS peut être égal à 1.

Cette base DB va également contenir la clé k commune à tous les modules de sécurité MS et permettant de décrypter le cryptogramme CY ainsi que l'indice N du nombre d'appariements précédemment exécutés.

Ce dernier est contenu initialement dans le module hôte MH dans une mémoire M qui peut être soit sécurisée, soit de type librement accessible. Il est tout de même préférable que cette mémoire soit protégée et difficilement accessible afin d'éviter qu'un appareil hôte ne se fasse passer pour un autre.

Ce cryptogramme CY est encrypté par la clé k et contient, dans une forme de réalisation, le numéro de série SN et une marque PT de valeur connue du module de sécurité. Cette marque PT permet au module de sécurité de s'assurer que le cryptogramme est valide. Cette marque PT est commune à tous les cryptogrammes. Selon une autre variante, elle peut être propre à l'appareil hôte. Le cryptogramme CY peut aussi contenir la clé d'appariement MHKey propre à l'appareil hôte, qui sera ensuite utilisée pour sécuriser la transmission d'informations entre le module MS et l'appareil hôte. Par exemple, une fois cette clé connue des deux modules, une clé de session KS peut être négociée et utilisée pour encrypter la communication. Bien entendu, dans un tel cas, la clé MHKey doit aussi être stockée dans la mémoire M de l'appareil hôte et cette mémoire doit donc être sécurisée.

Dans la base de données DB du module de sécurité MS, les données PDT1 à PDTn comprennent un compteur d'activité ou de chronologie tel que décrit plus haut. Rappelons que ces compteurs permettent de déterminer l'emplacement à remplacer au cas où tous les emplacements sont utilisés. Dans le cas où des compteurs d'activité sont utilisés, prenons l'exemple de trois emplacements, soit PDT1 à PDT3 respectivement occupés par des appariements effectués par des modules hôtes MHA, MHB et MHC. A chaque négociation d'un appariement entre le module de sécurité MS et le module MHC par exemple, le compteur CPT3 sera incrémenté.

Dans les formes d'exécution utilisant une clé de session KS générée à partir de la clé d'appariement KA, il est à noter que cet appariement peut évoluer dynamiquement c'est à dire que la clé de session KS est nécessairement changée après un certain temps d'utilisation; sur la base des éléments transmis lors de l'appariement entre ces deux entités (clé d'appariement, clé du module hôte MHKey), une nouvelle clé de session est générée. On peut dès lors compter le nombre de clés

de session déjà générées et considérer ce nombre comme compteur d'activité.

Lorsqu'une nouvelle demande d'appariement est requise au module de sécurité, il va déterminer le compteur d'activité le plus petit et libérer cet emplacement. Bien entendu, le module de sécurité contient aussi toute l'information nécessaire au calcul et à la vérification des codes secrets.

REVENDICATIONS

1. Méthode de contrôle d'appariement entre un premier dispositif tel qu'un module de sécurité amovible (MS) et un second dispositif tel qu'un appareil hôte (MH), cet appariement consistant à sécuriser l'échange des données à l'aide d'une clé d'appariement unique (KA), cette méthode consistant à :

- vérifier l'appariement entre les deux dispositifs et utiliser la clé d'appariement unique (KA) si l'appariement est déjà effectué, dans la négative,

- rechercher un emplacement (PDT) vide parmi les emplacements réservés aux données d'appariement dans le premier dispositif (MS) et dans l'affirmative,

- initier une procédure d'appariement en transmettant un cryptogramme (CY) contenu dans le second dispositif (MH), et contenant un identifiant (SN) propre à ce dispositif, ce cryptogramme étant encrypté par une clé secrète commune (k) à tous les premiers dispositifs,

- décrypter par le premier dispositif ce cryptogramme (CY) et en extraire l'identifiant (SN) du second dispositif,

- générer une clé d'appariement (KA) basée sur cet identifiant,

- mémoriser dans le premier dispositif (MS) les données de l'appariement avec le second dispositif.

2. Méthode selon la revendication 1, caractérisée en ce que la clé d'appariement (KA) est basée sur l'identifiant (SN) du second dispositif et les données propres au premier dispositif (MS).

3. Méthode selon les revendications 1 ou 2, caractérisée en ce que le cryptogramme (CY) est stocké dans le premier dispositif (MS) et encrypté avec une clé secrète commune aux seconds dispositifs (MH).

4. Méthode selon les revendications 1 à 3, caractérisée en ce que chaque emplacement (PDT) comprend un compteur d'activité (CPT) mis à jour à chaque vérification positive de l'appariement basé sur cet emplacement, la recherche de l'emplacement à remplacer étant déterminée sur la valeur du compteur d'activité (CPT).

5. Méthode selon les revendications 1 à 4, caractérisée en ce que l'appariement est conditionné à l'introduction d'un code secret (PIN) transmis au premier dispositif et vérifié par ledit premier dispositif.

6. Méthode selon la revendication 5, caractérisée en ce que le code secret est propre et unique à chaque premier dispositif (MS).

7. Méthode selon la revendication 5, caractérisée en ce que le code secret requis est différent à chaque appariement.

8. Méthode selon la revendication 5, caractérisée en ce qu'elle consiste à :

- transmettre un identifiant unique du premier dispositif et un identifiant unique du second dispositif à un centre de gestion,
- vérifier la conformité de cet appariement et calculer par le centre de gestion le code secret (PIN) correspondant sur la base des deux identifiants,
- transmettre à l'utilisateur ce code secret,
- initier l'appariement et requérir l'introduction du code secret (PIN), par le premier dispositif,
- calculer par le premier dispositif le code secret attendu sur la base des identifiants du premier et second dispositif,
- comparer le code calculé avec celui introduit par l'utilisateur,
- accepter l'appariement si les deux codes sont identiques.

9. Méthode selon la revendication 8, caractérisée en ce qu'elle consiste à déterminer le nouveau code secret sur la base des deux identifiants et d'un indice (N) représentant le nombre d'appariement antérieurement exécuté, le premier dispositif conservant en mémoire cet indice (N).

ABREGE

Le but de la présente invention est d'apparier un module de sécurité avec un ou plusieurs appareils hôtes dans un environnement dans lequel le module hôte ne dispose pas de liaison avec un centre de gestion.

Ce but est atteint par une méthode de contrôle d'appariement entre un premier dispositif tel qu'un module de sécurité amovible et un second dispositif tel qu'un appareil hôte, cet appariement consistant à sécuriser l'échange des données à l'aide d'une clé d'appariement unique, cette méthode consistant à :

- vérifier l'appariement entre les deux dispositifs et utiliser la clé d'appariement unique si l'appariement est déjà effectué, dans la négative,
- rechercher un emplacement vide parmi les emplacements réservés aux données d'appariement dans le premier dispositif et dans l'affirmative,
- initier une procédure d'appariement en transmettant un cryptogramme contenu dans le second dispositif, et contenant un identifiant propre à ce dispositif, ce cryptogramme étant encrypté par une clé secrète commune à tous les premiers dispositifs,
- décrypter par le premier dispositif ce cryptogramme et en extraire l'identifiant du second dispositif,
- générer une clé d'appariement basée sur cet identifiant,
- mémoriser dans le premier dispositif les données de l'appariement avec le second dispositif.

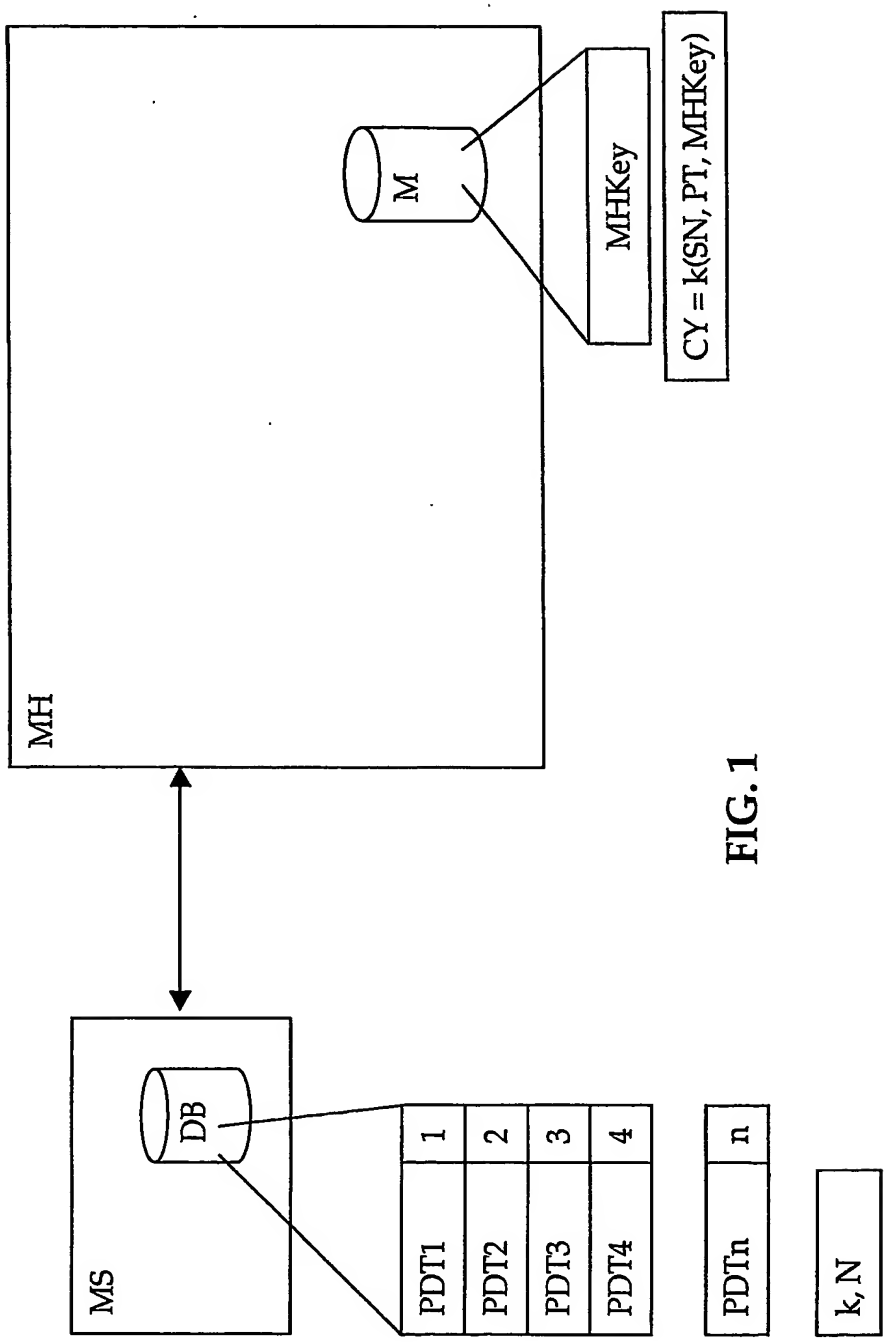

MH
M
MHKey
CY = k(SN, PT, MHKey)
MS
DB
1
2
3
4
PDT1
PDT2
PDT3
PDT4
n
PDTn
k, N

FIG. 1